



Statewide Incident Response Review





"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.



Cyber Security Awareness Website

- Contains useful information with helpful links
- The governor's proclamation is available to view
- Links for children and keeping them safer online
- Links to Free Security Training (*i.e. no cost*)
- Website address is:

<http://www.esrmo.scio.nc.gov/CyberSecurity/default.aspx>

The screenshot shows the North Carolina Cyber Security Awareness website. At the top, there is a logo for "Cyber Security awareness state of north carolina" and a navigation bar with links for "NC Gov | ITS | ESRMO | Contact Us". Below the header, there is a "Cyber Security Tips" section with links for "Hot Links", "Rebroadcast Webcasts", "For Kids", "Newsletters", and "Contact Us". To the right of this is a large graphic with a computer monitor, a padlock, and the text "Cyber Security is our shared responsibility... Always Stop, Think before you Connect." Below the tips section, there is a "cyber security tips" section with a list of tips, including "Use up to date 'anti-virus software'", "Do not open e-mail from unknown sources", "Use 'hard to guess' passphrases", "Protect your computer files with a 'firewall'", "Don't share your computer with strangers - 'peer to peer file sharing'", "Update your computer's operating system and applications regularly", "Shut down your computer when not in use", "Use Instant Messengers/Chat wisely", "Make sure you know what to do in the event of a computer infection", "Regularly back-up your computer data", "Use encryption products to protect data", and "Take advantage of security features in wireless access points". To the right of the tips is a "welcome" section with a paragraph about the site's purpose. Below the welcome section is a "hot links" section with a list of links, including "Governor Perdue's Proclamation", "State CIO Worker's Memo", "US-CERT", "Home Network Security", "Coordinating Virus and Spware Defense", "Safeguarding your Data", "Multi-State Information Sharing Analysis Center (MS-ISAC)", "NC Computer Protection", "CERT Advisories", "SANS Incidents", "Information Security Incident Reporting", "MS-ISAC Calendar 2012", and "MS-ISAC Calendar 2013". To the right of the hot links is a "rebroadcast webcasts" section with a list of webcasts, including "Our Shared Responsibility - The Strategy for Promoting CyberSecurity Awareness", "Cloud Computing -- 'Security Considerations You Should Know'", "Phishing Scams -- Don't Get Hooked (Part I of II)", "Phishing Scams -- Don't Get Hooked (Part II of II)", "Keeping Your Broadband Internet Connection Secure", "Mobile Security and Encryption", and "Security 101 for Your PC". At the bottom of the page, there is a "tip of the day" section with a link to "Shop Safely Online", an "advisories" section with a link to "Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (MS012-064)", and a "4kids" logo. The footer of the website includes logos for "4kids", "TAKE A BITE OUT OF CYBER CRIME", "NETSMARTZ KIDS", "iKeepSafe", and "4KIDS.ORG".





Cyber Security Pledge

- Stop, and Think (consider appropriateness and risk) before I Connect to the Internet.
- Take personal responsibility for security, follow my agency's security policies.
- Work to the best of my ability to keep my agency's staff, property and information safe and secure.
- Promptly report all security incidents or concerns to my organization's security office or other appropriate contact.
- Spread the message to my friends, co-workers and community about staying safe online.
- Website address is:

<http://www.esrmo.scio.nc.gov/CyberSecurity/default.aspx>





Cyber Security: What is it?

- **Cyber Security (computer security)** is a branch of information security that applies to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, unauthorized access, or natural disaster, while allowing the information and property to remain accessible and productive to the intended users.





Security Incident

An information security incident is an **adverse** event or a threat of an adverse event where an information technology resource is:

- Accessed or used without authorization
- Attacked or threatened with attack
- Used in a manner inconsistent with established laws or policy with the potential to cause the real or possible loss of *confidentiality, integrity, or availability* of the resource or its information
- Breached or threatens to breach the accountability, or auditability of the resource or its information.





Reportable Incidents

E-Mail

- SPAM
- Open Relay Complaints
- DOS against Mail servers
- E-mail Harassment
- Spam BOT
- Phishing (Social Engineering)





Reportable Incidents

Hacking

- Port scanning
- Unauthorized access
- SQL Injection
- Warez Servers
- Anonymous Proxies
- Web Defacements
- Denial of Service (DOS)
- Brute Force Attacks
- System Compromise



Malicious Software (aka. Malware)

- Malware Outbreaks
 - Multiple systems/users reporting infection
- AV Failures (Large Scale)
 - Fail to detect
 - Fail to clean
- Vectors of Infection
 - Hostile websites
 - Malicious email/text/social networking links





Reportable Incidents

Inappropriate Use

- Copyright violations (Peer-to-Peer Networks – Kaaza, Gnutella, Torrents)
- Downloading and/or distribution of pornography
- Unauthorized access to remote system/account by state employee
- Use of state resources for personal gain or harassment





Reportable Incidents

Other

- Law Enforcement Issues
 - Intelligence
 - Theft and Fraud
 - Stalking
 - Harassing Telephone Calls
- Data loss (Desktops, laptops, portable media, etc.)
 - *When reporting these incidents, you must note if the device and/or media contained PII and if the device/data was protected with encryption.*
- Miscellaneous incidents not covered above!





Agency Responsibilities

G.S. § 147-33.113(a) requires agency heads to:

- Provide details of information technology security employed at the agencies
- Report computer related security incidents to the State CIO within 24 hours
- Designate an agency security liaison to coordinate with the State CIO

The General Assembly, Judicial Department, and the University of North Carolina system are exempt, but may choose to comply.





How do I report an incident?

- Three Methods for reporting cyber incidents:
 - Report the incident using the online incident reporting form at <https://incident.its.state.nc.us> *
 - Open a ticket with the ITS Service Desk *
 - Ask for it to be routed to ESRMO/Threat Management
 - Contact a member of the ESRMO Threat Management Team directly

**If you need immediate assistance, please contact a member of the Threat Management team directly.*





How do I report an incident?

- Report cyber incidents at <https://incident.its.state.nc.us>
- What ESRMO submits on the agency's behalf:
 - Malware notifications ESRMO sends to the agency
 - Spam notifications ESRMO sends to the agency
 - Copyright Infringement notifications ESRMO sends to the agency
- All other cyber incidents should be submitted by the agency.

Information Systems Incident Reporting WSIS - Mozilla Firefox

Enterprise Security and Risk Management Office
STATE OF NORTH CAROLINA
George Bakolia, State CIO

Information Security Incident Reporting

This website is for reporting information security incidents involving information systems located on the State of North Carolina Wide Area Network (NCWAN). This form may be used by State personnel to comply with reporting requirements as directed by N.C.G.S. § 147-33.82(f) or by persons reporting incidents in which a system located on the NCWAN was used to attack or infect a system outside of the NCWAN.

Incident Reporting

To report an information security incident to the State of North Carolina Office of Enterprise Security & Risk Management please complete the form below.

Please contact the Customer Support Center at 1-800-722-3946 for questions about reporting an incident, or if you need an Information Security Officer to contact you immediately.

The information provided by State agencies to the State Chief Information Officer under this subsection is protected from public disclosure pursuant to N.C.G.S. § 132-6.1(c).

If additional information is required, you will be contacted directly.

Required Items

Point of Contact (POC) Information

Report Date / Time: 9/21/2009 11:27:51 AM

First Name **

Last Name **

Title

Work Telephone Number **

Extension

Cell Phone/After Hours

E-mail Address **

Agency: -- Select an agency/Dept --

Division

Organizational Business Name

Address: Street **

City **

State ** North Carolina

Zip Code **

Incident Information

1. Name of Organization: -- Select an agency/Dept --

Done





Questions?